



# UNITED STATES PATENT AND TRADEMARK OFFICE

25  
UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/030,255	01/09/2002	Michel Hazard	T2146-907683	8944
7590	02/13/2004		EXAMINER	
Edward J. Kondracki Miles & Stockbridge Suite 500 1751 Pinnacle Drive McLean, VA 22102-3833			NGUYEN, NAM V	
			ART UNIT	PAPER NUMBER
			2635	A
			DATE MAILED: 02/13/2004	

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/030,255	HAZARD, MICHEL	
	<b>Examiner</b>	<b>Art Unit</b>	
	Nam V Nguyen	2635	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 09 January 2002.
- 2a) This action is FINAL.                    2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-15 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 1-15 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 09 January 2002 is/are: a) accepted or b) objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. §§ 119 and 120

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some \* c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.
- 13) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.
- a) The translation of the foreign language provisional application has been received.
- 14) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

#### Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2 .
- 4) Interview Summary (PTO-413) Paper No(s) \_\_\_\_\_ .
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: \_\_\_\_\_

## **DETAILED ACTION**

The application of Hazard for a "method for authenticating a portable object, corresponding portable object, and apparatus therefor" filed January 9, 2002 has been examined.

This application claims foreign priority based on the application 00/05894 filed May 09, 2000 in France. Receipt is acknowledged of papers submitted under 35 U.S.C 119(a) – (d), which papers have been placed of record in the file.

This application claims priority to a 371 of PCT/FR01/01359, which is filed on May 04, 2001.

A preliminary amendment to the specification and claims 1-15 have been entered and made of record.

Claims 1-15 are pending.

### *Specification*

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

The current abstract using phrase “means” is implied and should be avoided. See MPEP 608.01(b).

Appropriate correction is required.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-4, 9-10 and 12-15 are rejected under 35 U.S.C. 102(b) as being anticipated by Kruse et al. (US# 4,786,790).

Referring to claims 1, 9, 12 and 14, Kruse et al. disclose a data exchange system with authentication code comparator as recited in claims 1, 9, 12 and 14. See Figures 1-2 and respective portions of the apparatus and method.

Kruse et al. disclose a method for authenticating a portable object (KK) (i.e. customer card) including information processing means (fs) and information storage means (P and KPC) (column 2 lines 20 to 66; column 3 line 27 to 32; see Figure 1), the information storage means (P) containing at least one code (i.e. a proper program) defining operation steps capable of being executed by the portable object (KK) (column 2 lines 20 to 53), as well as a one-way function (column 2 line 54 to column 3 line 13), comprising sending the portable object (KK) an order for executing a calculation of a result by applying to said one-way function at least part of said code

and using said result to decide whether or not the portable object (KK) is authentic (column 2 lines 60 to column 3 line 44).

Referring to claim 2, Kruse et al. disclose a method according to claim 1, wherein said result enters into the implementation of a predetermined operation, said operation being performed successfully only when the portable object is authentic (column 2 lines 60 to column 3 line 9; see Figures 1-2).

Referring to claim 3, Kruse et al. disclose a method according to claim 2, wherein said predetermined operation comprises a decryption operation, said result making it possible to produce an associated decryption key (column 2 lines 60 to column 3 line 9; see Figures 1-2).

Referring to claims 4, 10, 13 and 15, Kruse et al. disclose a method according to claims 2, 9, 12 and 14, wherein said part of said code used in the calculation, comprises a machine code (i.e. programming code) (column 2 lines 20 to 66).

#### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

- (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 5, 8 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kruse et al. (US# 4,786,790) as applied to claim 1 above, and in view of Anders et al. (US# 4,656,463).

Referring to claims 5 and 11, Kruse et al. disclose a method according to claims 1 and 9, however, Kruse et al. did not explicitly disclose further comprising wherein the portable object contains a real code defining operations designed to be executed by the portable object, and a dummy code defining operations not designed to be executed by the portable object, said code used in the calculation of a result comprising a dummy code.

In the same field of endeavor of access communication system, Anders et al. teach that the portable object (182) (i.e. an active transceiver) contains a real code (i.e. programming codes) defining operations designed to be executed by the portable object (column 12 lines 51 to column 13 line 52; see Figure 13), and a dummy code (i.e. uncoded sectors) defining operations not designed to be executed by the portable object (182), said code (i.e. programming codes) used in the calculation of a result comprising a dummy code (uncoded sectors) (column 42 lines 43 to 59; see Figure 33) in order to obtain the best individual codes necessary for the operation of each individual system.

One of ordinary skilled in the art recognizes the need to generate programming codes of a tag having a particular code is not used with an uncoded sector of Anders et al. in a program authentication codes of a customer card of Kruse et al. because Kruse et al. suggest it is desired to provide that programming secret code in a protected, programmable read only memory from a specific chip card (column 2 line 60 to column 3 line 9) and Anders et al. teach that an individual codes for the operation of each system is filled with a dummy code in an allocated area if an

individual codes is not used in a particular system in order to increase the difficulty of decoding the source code. Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to generate programming codes of a tag having a particular code is not used with an uncoded sector of Anders et al. in a program authentication codes of a customer card of Kruse et al. with the motivation for doing so would have been to provide more secure method for authorization of a user.

Referring to claim 8, Kruse et al. in view of Anders et al. disclose a method according to claim 1, Anders et al. disclose wherein said code comprises a set of binary words, said code used in the calculation being defined by a subset of said binary words comprising binary words distributed in the information storage means at a determined pitch, said pitch being sent to the portable object (column 14 lines 7 to 36).

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kruse et al. (US# 4,786,790) as applied to claim 1 above, and in view of Camion et al. (US# 6,167,516).

Referring to claim 6, Kruse et al. disclose a method according to claim 1, however, Kruse et al. did not explicitly disclose further comprising repeatedly sending said order to the portable object during its life, prior to execution by the portable object of said operation steps.

In the same field of endeavor of authentication device, Camion et al. teach that repeatedly sending said order to the portable object (1) during its life, prior to execution by the portable

object (1) of said operation steps (column 9 line 51 to 55; column 11 line 31 to 51; see Figures 3-6) in order to restart calculation and to proceed to a new extraction of a word from a memory.

At the time the invention, it would have been obvious to a person of ordinary skill in the art to recognize the need for repeatedly until proceed to a new extraction of a word from source memory in the method of verifying data exchange system with authentication code comparator of Kruse et al. because repeatedly verifying for authentication of customer card would improve the reliable and secure communication between a chip card and a terminal that has been shown to be desirable in the data exchange system of Kruse et al.

Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kruse et al. (US# 4,786,790) as applied to claim 1 above, and in view of Nolan (US# 4,896,261).

Referring to claim 7, Kruse et al. disclose a method according to claim 1, however, Kruse et al. did not explicitly disclose wherein said code used in the calculation is defined by a start address and an end address in the information storage means, and further including the step of sending said start and end addresses to the portable object.

In the same field of endeavor of authentication device, Nolan teaches that code (i.e. message) used in the calculation is defined by a start address and an end address in the information storage means (22) (i.e. memory), and further including the step of sending said start and end addresses to the portable object (15) (i.e. control module) (column 1 line 58 to column 2 line 21; column 4 lines 45 to 63; column 5 lines 10 to 29; see Figures 1-2) in order to identify each message was sent to the processor.

At the time the invention, it would have been obvious to a person of ordinary skill in the art to recognize to have a message sent to the control module having a start and end message address in key code programmable read only memory to process an authentication code of Kruse et al. because having a start and end address would distinguish the message from other message in the memory in order to improve reliable and secure communication between a chip card and a terminal that has been shown to be desirable in the data exchange system of Kruse et al.

### ***Conclusion***

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Leonardi (US# 6,556,680) discloses a method for authorization check.

Linder (US# 6,363,151) discloses a method and system for subscriber authentication and/or encryption of items of information.

Juopperi (US# 6,225,888) discloses an authentication between communicating parties in a telecommunications network.

Mills (US# 6,198,823) discloses a method for improved authentication for cellular phone transmissions.

Iijima (US# 5,225,664) discloses a mutual authentication system.

Ogasawara et al. (US# 5,097,115) disclose a transaction authentication system.

Art Unit: 2635

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nam V Nguyen whose telephone number is 703-305-3867. The examiner can normally be reached on Mon-Fri, 8:30AM - 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael Horabik can be reached on 703-305-4704. The fax phone numbers for the organization where this application or proceeding is assigned are 703-872-9314 for regular communications and 703-872-9314 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Nam Nguyen  
February 7, 2004



MICHAEL HORABIK  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2600

